CLAIMS

What is Claimed is:

1. A method of storing program material for subsequent replay, comprising the steps of:

receiving a data stream comprising the program material encrypted according to a first encryption key and control data, the control data comprising the first encryption key and being encrypted;

further encrypting the encrypted program material according to a second encryption key;

encrypting the second encryption key according to a third encryption key to produce a fourth encryption key; and

storing the further encrypted program material and control data and the fourth encryption key.

2. The method of claim 1, further comprising the steps of:

retrieving the stored further encrypted program material, control data and the fourth encryption key;

decrypting the fourth encryption key using the third encryption key to produce the second encryption key;

decrypting the further encrypted program material with the second encryption key to produce the encrypted program material;

decrypting the control data to produce the first encryption key; and

decrypting the encrypted program material using the first encryption key.

3. The method of claim 2, further comprising the steps of:

accepting a PPV request before decrypting the encrypted program material using the first encryption key; and

recording billing information regarding the program material.

4. The method of claim 2, further comprising the steps of:

further encrypting the control data according to the second encryption key;

storing the further encrypted control data; and

decrypting the further encrypted control data according to the second encryption key.

5. The method of claim 2, further comprising the step of providing the program material to a presentation device.

6. The method of claim 2, wherein the data stream is received in a receiver and the third key is unique to the receiver.

7. The method of claim 6, wherein the second key is unique to the receiver.

8. The method of claim 1, wherein the further encrypted program material, the control data and the third encryption key are stored on a disk drive device.

9. The method of claim 8, wherein the disk drive device is a hard disk drive.

10. The method of claim 8, wherein the disk drive device is an optical disk drive.

11. The method of claim 1, wherein the data stream further comprises metadata describing program material replay rights.

12. The method of claim 11, wherein the second encryption key is derived at least partially from the metadata.

13. The method of claim 12, wherein the second encryption key is derived at least partially from the broadcast time of the program material.

14. The method of claim 13, further comprising the step of augmenting the second encryption key with at least a portion of the metadata before encrypting the second encryption key according to the third encryption key.

15. The method of claim 14, further comprising the steps of:

retrieving the stored further encrypted program material, control data and the fourth encryption key;

decrypting the fourth encryption key using the third encryption key to produce the second encryption key and the portion of the metadata;

decrypting the further encrypted program material with the second encryption key to produce the encrypted program material;

accepting a PPV request; and

determining if the PPV request is permitted using the portion of the metadata; and

decrypting the control data to produce the first encryption key and decrypting the encrypted program material using the first encryption key if the PPV request is permitted.

16. A receiver for storing program material for subsequent replay, comprising:

a tuner, for receiving a data stream comprising encrypted access control information and the program material encrypted according to a first encryption key, the access control information including the first encryption key;

a first encryption module, communicatively coupled to the tuner and communicatively coupleable to a media storage device, for further encrypting the encrypted program material according to a second encryption key and for encrypting the second encryption key according to a third encryption key to produce a fourth encryption key;

a first decryption module communicatively coupleable to the media storage device, for decrypting the fourth encryption key retrieved from the media storage device using the third encryption key to produce the second encryption key, and for decrypting the further encrypted program material retrieved from the media program device to produce the encrypted program material;

a conditional access module communicatively coupled to the first decryption module, for decrypting the encrypted access control information to produce the first encryption key; and

a second decryption module, for decrypting the program material using the first encryption key.

17. The apparatus of claim 16, further comprising a media storage device communicatively coupled to the first encryption module and the first decryption module, for storing and retrieving the further encrypted program material and the control data and the fourth encryption key.

18. The apparatus of claim 16, wherein:

the first encryption module further encrypts the encrypted access control information according to the second encryption key; and

the first decryption module further decrypts the further encrypted access control information according to the second encryption key.

19. The apparatus of claim 18, further comprising:

a user I/O device for accepting a viewing request; and

a purchase history module for accepting and storing billing information regarding the program material.

20. The apparatus of claim 19, wherein the conditional access module decrypts the encrypted access control information in response to the acceptance of a viewing request.

21. The receiver of claim 17, wherein the second encryption key and the third encryption key are receiver-unique.

22. The receiver of claim 17, wherein the first decryption module and the first encryption module are implemented in a single chip device.

23. A method of storing program material for subsequent replay, comprising the steps of:

accepting a received data stream comprising the program material encrypted according to a first encryption key and control data, the control data comprising the first encryption key and being encrypted;

further encrypting the encrypted program material according to a second encryption key;

encrypting the second encryption key according to a third encryption key to produce a fourth encryption key; and

providing the further encrypted program material and control data and the fourth encryption key for storage.

24. An apparatus for storing program material for subsequent replay, comprising:

means for accepting a received data stream comprising the program material encrypted according to a first encryption key and control data, the control data comprising the first encryption key and being encrypted;

means for further encrypting the encrypted program material according to a second encryption key;

means for encrypting the second encryption key according to a third encryption key to produce a fourth encryption key; and

means for providing the further encrypted program material and control data and the fourth encryption key for storage.

25. An apparatus for storing program material for subsequent replay, comprising:

means for receiving a data stream comprising the program material encrypted according to a first encryption key and control data, the control data comprising the first encryption key and being encrypted;

means for further encrypting the encrypted program material according to a second encryption key;

means for encrypting the second encryption key according to a third encryption key to produce a fourth encryption key;

means for storing the further encrypted program material and control data and the fourth encryption key.

26. The apparatus of claim 25, further comprising:

means for retrieving the stored further encrypted program material, control data and the fourth encryption key;

means for decrypting the fourth encryption key using the third encryption key to produce the second encryption key;

means for decrypting the further encrypted program material with the second encryption key to produce the encrypted program material; and

means for decrypting the control data to produce the first encryption key; and

means for decrypting the encrypted program material using the first encryption key.

27. The apparatus of claim 25, further comprising:

means for accepting a PPV request before decrypting the encrypted program material using the first encryption key; and

means for recording billing information regarding the program material.

28. The apparatus of claim 25, further comprising:

means for further encrypting the control data according to the second encryption key;

means for storing the further encrypted control data; and

means for decrypting the further encrypted control data according to the second encryption key.

29. The apparatus of claim 25, further comprising means for providing the program material to a presentation device.

30. The apparatus claim 25, wherein the data stream is received in a receiver and the third key is unique to the receiver.

31. The apparatus of claim 30, wherein the second key is unique to the receiver.

32. The apparatus of claim 25, wherein the further encrypted program material, the control data and the third encryption key are stored on a disk drive device.

33. The apparatus of claim 32, wherein the disk drive device is a hard disk drive.

34. The apparatus of claim 31, wherein the disk drive device is an optical disk drive.

35. The apparatus of claim 25, wherein the data stream further comprises metadata describing program material replay rights.

36. The apparatus of claim 35, further comprising means for augmenting the second encryption key with at least a portion of the metadata before encrypting the second encryption key according to the third encryption key.

37. The apparatus of claim 36, further comprising:

means for retrieving the stored further encrypted program material, control data and the fourth encryption key;

means for decrypting the fourth encryption key using the third encryption key to produce the second encryption key and the portion of the metadata;

means for decrypting the further encrypted program material with the second encryption key to produce the encrypted program material;

means for accepting a PPV request; and

means for determining if the PPV request is permitted using the portion of the metadata; and

means for decrypting the control data to produce the first encryption key and decrypting the encrypted program material using the first encryption key if the PPV request is permitted.